UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

MARITZ HOLDINGS INC.,)
)
Plaintiff,)
)
vs.) Case No. 4:18-CV-826 CDP
)
COGNIZANT TECHNOLOGY)
SOLUTIONS U.S. CORPORATION,)
)
Defendant.)

MEMORANDUM AND ORDER

In 2016 and 2017, plaintiff Maritz Holdings was the victim of phishing cyberattacks which led to unknown perpetrators obtaining over $12 million dollars' worth of reward gift cards. An investigation into the 2017 cyberattack allegedly revealed a connection to account credentials that Maritz had issued to employees of its IT services provider, defendant Cognizant Technology Solutions U.S. Corporation. Maritz brings this suit alleging that Cognizant violated the federal and Missouri computer tampering statutes and breached its contract in a number of ways. Maritz also alleges tort claims of conversion, negligence and unjust enrichment.

Cognizant moves to dismiss the complaint, arguing that Maritz has failed to allege that any Cognizant employee committed any of the cyberattacks and that Maritz cannot state claims against it under any of the theories set out in the complaint. I will grant the motion to dismiss as to the two statutory computer tampering claims and as to the conversion claim (Counts I, II and III). I also agree that Maritz cannot obtain the remedy of an accounting as part of its unjust enrichment claim, and so I will dismiss that claim for relief from Count VI. The motion is denied as to Maritz's remaining breach of contract, negligence, and unjust enrichment claims.

Factual Background

Maritz designs and operates customer rewards programs for corporate clients. In connection with these programs, Maritz purchases redeemable electronic gift cards and stores them in its internal computer system before issuing the gift cards to program participants. Maritz alleges its system was targeted in two successful cyberattacks in March 2016 and February 2017.

In the March 2016 attack, an unidentified perpetrator directed three rounds of phishing emails to more than two hundred Maritz employees. The emails contained a corrupted file which, when loaded, installed a concealed "backdoor" in the target computer. The backdoor granted the perpetrator broad access to Maritz's internal computer system, allowing the perpetrator to download and redeem gift cards worth more than $11 million. Maritz's investigation into the 2016 attack could not determine the sources of the phishing emails and subsequent theft.

The February 2017 cyberattack unfolded in similar fashion. As before, an unidentified perpetrator sent phishing emails to Maritz employees. The phishing emails contained a malicious link that installed concealed remote access tools in several Maritz computers, granting the perpetrator unfettered and undetected access to Maritz's internal computer system. Among other confidential information, the perpetrator harvested access credentials for Maritz' card fulfillment system, and allegedly stole an additional $1.2 million in unissued gift cards. Maritz again investigated the attack; unlike the first, this investigation revealed several links to Cognizant employees.

Cognizant and Maritz had entered into an Offshore Contracting Master Services Agreement (the "MSA") in 2010 to provide IT support and outsourcing services.[1] Cognizant employees were issued individual accounts with limited access to Maritz's computer system and databases. Maritz's investigation into the 2017 attack revealed the attackers were accessing the Maritz system using account credentials registered to Cognizant. The investigation also uncovered a third hacking attempt tied to a Cognizant account, and revealed that Cognizant employees had shared their account credentials in violation of Maritz company

[1] Because Maritz attached the MSA as an exhibit to its complaint, the MSA is considered "a part of the pleading for all purposes" under Rule 10(c), and I may consider it in my analysis of Cognizant's motion to dismiss. MSA, ECF 1, Ex. 1; Fed. R. Civ. P. 10(c).

policy. Based on this information, Maritz concluded that Cognizant employees were responsible for the February 2017 phishing attack and gift card theft.

Maritz's investigation additionally revealed that the same program was used by the perpetrator in both the 2017 and 2016 attacks, and that the 2017 attack showed similarities to the 2016 attack. Maritz ultimately concluded that the same Cognizant employees implicated in the February 2017 attack were also responsible for the larger March 2016 attack.

Maritz thereafter filed this case against Cognizant alleging one violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, one violation of the Missouri Computer Tampering Statute (MCTS), Mo. Rev. Stat. § 569.095, and one count each of conversion, breach of contract, negligence, and unjust enrichment. Cognizant denies that its employees had any involvement in the attacks, and now moves to dismiss each count under Rule 12(b)(6), Fed. R. Civ. P.

Discussion

The purpose of a motion to dismiss under Rule 12(b)(6) of the Federal Rules of Civil Procedure is to test the legal sufficiency of the complaint. To survive a 12(b)(6) motion, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief "that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* Although a complaint need not contain "detailed factual allegations," it must allege facts with enough specificity "to raise a right to relief above the speculative level." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "A well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of those facts is improbable, and 'that a recovery is very remote and unlikely.'" *Id.* at 556 (internal citation omitted).

Cognizant argues that Maritz has made no plausible allegations that would show that it or its employees were responsible for the cyberattacks. However, on this motion to dismiss, I must assume the truth of Maritz's factual allegation that "the attackers were accessing the Maritz system using accounts registered to Cognizant" in relation to the 2017 attack. This allegation gives rise to a reasonable inference that a Cognizant employee was responsible for the 2017 hacking. Further, based on Maritz's allegations that the second attacker had used the same program and "had run searches . . . for certain words and phrases connected to the Spring 2016 attack," a reasonable inference can be drawn that the same perpetrator committed the two attacks. ECF 1 at ¶ 42. Accordingly, because Maritz has plausibly alleged a Cognizant employee committed the 2017 gift card theft, and alleged facts from which a reasonable inference can be drawn that the same perpetrator committed the 2016 theft, I will deny Cognizant's motion to dismiss to the extent it challenges the facial plausibility of Maritz's allegations.

Counts I, II, and III: Computer Fraud and Conversion

Count I of Maritz's complaint is brought under the federal CFAA, 18 U.S.C. § 1030. Count II is brought under Missouri's analogous computer tampering statute, Mo. Rev. Stat. § 569.095. Both computer tampering statutes provide civil remedies to owners of protected computers who are injured by one who accesses computers, or modifies or discloses data, without authorization or by exceeding the perpetrator's authorization. 18 U.S.C. § 1030(g); Mo. Rev. Stat. § 569.095, § 537.525. The federal statute provides the remedy against "the violator," while the state law provides the remedy against "any person who violates" the law. *Id.*

In both counts, and in Maritz's common-law conversion claim in Count III, Maritz alleges that one or more Cognizant employees accessed Maritz's network without authorization (or exceeded their authorized access) and improperly removed confidential data. Maritz alleges that Cognizant is vicariously liable for the acts of its employees because, based "on information and belief," the Cognizant employees committed the hacking "while acting in the scope of their employment and under the control and supervision of Cognizant." ECF 1 at ¶ 50.

Maritz complaint, however, fails to allege any facts that could plausibly support its conclusory allegation that the Cognizant employees' unlawful acts fell within the course and scope of employment.[2]

Under the doctrine of *respondeat superior*, an employer may be held vicariously liable for its employee's misconduct where that employee is acting within the course and scope of his employment. *Tuttle v. Muenks,* 964 S.W.2d 514, 517 (Mo. Ct. App. 1998). "The course and scope of employment is defined as acts (1) which, even though not specifically authorized, are done to further the business or interests of the employer under his 'general authority and direction' and (2) which naturally arise from the performance of the employer's work." *Hilyard v. Medtronic, Inc*., 21 F. Supp. 3d 1012, 1016 (E.D. Mo. 2014) (quoting *Daugherty v. Allee's Sports Bar & Grill*, 260 S.W.3d 869, 872-73 (Mo. Ct. App. 2008)). The plaintiff has the burden of proving that an employee's tortious conduct was within the course and scope of his employment. *Ewing–Cage v.*

[2] Some courts have outright declined to recognize vicarious liability claims under the CFAA's civil provision, *see Doe v. Dartmouth-Hitchcock Med. Ctr.*, No. CIV. 00-100-M, 2001 WL 873063, at *5 (D.N.H. July 19, 2001), while other courts apply a heightened vicarious liability standard to CFAA claims. *See, e.g., Butera & Andrews v. Int'l Bus. Machines Corp.*, 456 F. Supp. 2d 104, 113 (D.D.C. 2006) (dismissing vicarious liability claim because plaintiff failed to present evidence that the company "tacitly knew and approved of the conduct allegedly engaged in by its employees or agents."). I need not determine whether Maritz's computer tampering claims are precluded as a matter of law, nor whether to apply a heightened vicarious liability standard, because Maritz's claims cannot withstand scrutiny even under Missouri's traditional *respondeat superior* principles.

Quality Productions, Inc., 18 S.W.3d 147, 150 (Mo. Ct. App. 2000) (citation omitted). A conclusory allegation that an employee's acts fall within the scope of employment is not sufficient to meet plaintiff's burden. *Oetting v. Heffler, Radetich & Saitta, LLP*, No. 4:11-CV-253 CEJ, 2011 WL 3055235, at *3 (E.D. Mo. July 25, 2011).

Maritz's vicarious liability claims fail both prongs of Missouri's *respondeat superior* test. First, Maritz simply does not allege that the Cognizant employee perpetrator was serving Cognizant's interests in committing the hacking and conversion. This omission alone constitutes grounds to dismiss Maritz's vicarious liability claims. *See Oetting*, 2011 WL 3055235, at *4 (dismissing vicarious liability claim where plaintiff failed to allege the defendant's employee was serving his employer's interests in filing fraudulent claims).

Moreover, Maritz does not allege any facts from which a reasonable inference could be drawn that the hacker's actions were done to benefit Cognizant's interests. *See, e.g., Pac. Aerospace & Elecs., Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1192–1193 (E.D. Wash. 2003) (vicarious liability imposed where a corporate defendant hired competitor's employees who misappropriated trade secrets and confidential information). To the contrary, Maritz has alleged that a Cognizant employee secretly infiltrated a longstanding client's computer system and stole over $12 million in redeemable gift cards, which directly contradicts Cognizant's contractual obligations under the MSA[3] and could expose the company to serious criminal and civil liability. Accordingly, even if a Cognizant employee were responsible for the hacking and conversion, Cognizant could not be held vicariously liable for its employee's wrongdoing. *See Bradley v. Transportation Sec. Admin.*, 552 F. Supp. 2d 957, 961 (E.D. Mo. 2008) (internal citation omitted) ("[F]or an employer to be liable, the employee's … wrongful conduct must not arise wholly from some external, independent, or personal motive.").

Further, Maritz's claims fail under the second prong of Missouri's *respondeat superior* test because the hacking and conversion did not "naturally arise" from the performance of the alleged Cognizant employee perpetrator's work. *Daugherty*, 260 S.W.3d. at 273. "'Naturally' implies that the employees' conduct must be usual, customary, and expected. This amounts to a requirement of foreseeability." *Id*. Vicarious liability is rarely imposed on an employer when its employee commits a serious crime because such acts are generally considered unforeseeable as a matter of law:

[3] Among other things, Cognizant guaranteed that "all Outsourced Services [would] be . . . performed in compliance with applicable laws, rules and regulations," and that it would "keep all Confidential Information strictly confidential." ECF 1 at ¶¶ 15, 17.

> The fact that the servant intends a crime, especially if the crime is of some magnitude, is considered in determining whether or not the act is within the employment, since the master is not responsible for acts which are clearly inappropriate to or unforeseeable in the accomplishment of the authorized result. The master can reasonably anticipate that servants may commit minor crimes in the prosecution of the business, but serious crimes are not only unexpectable but in general are in nature different from what servants in a lawful occupation are expected to do.

Oetting, 2011 WL 3055235, at *4 (quoting *Wellman v. Pacer Oil Co.*, 504 S.W.2d 55, 58 (Mo. banc 1973)). Maritz's allegations accuse the Cognizant employee of conduct that is a crime under both the federal and Missouri computer tampering statutes. *See* 18 U.S.C. §1030(c)(2)(B); Mo. Rev. Stat. § 569.095(2). Additionally, conversion, as alleged in Count III, is a crime in Missouri and punishable by imprisonment for a term of three to ten years. Mo. Rev. Stat. § 570.030(4); Mo. Rev. Stat. § 558.011(3). These felony offenses cannot be considered "usual, customary, and expected" facets of a Cognizant employee's job duties, nor could Cognizant have reasonably foreseen that its employee would engage in the alleged misconduct. Cognizant's motion to dismiss Counts I, II, and III is therefore granted.

Count IV: Breach of Contract

In Count IV, Maritz alleges Cognizant violated its contractual obligations under the MSA in four distinct ways: 1) by failing to prevent its employees or other unauthorized personnel from improperly accessing Maritz's systems; 2) by failing to "take responsibility" for the security breaches; 3) by failing to prevent its employees from sharing Cognizant account credentials and usernames; and 4) by improperly billing Maritz for the service time its employees spent engaging in the cyberattacks. Cognizant moves to dismiss each distinct theory for failure to state a claim.

To state a cause of action for breach of contract, a plaintiff must allege: "(1) the making and existence of a valid and enforceable contract, (2) the right of the plaintiff and the obligation of the defendant thereunder, (3) a violation thereof by the defendant, and (4) damages resulting to the plaintiff from the breach." *Compass Bank v. Eager Rd. Assocs., LLC*, 922 F. Supp. 2d 818, 822–23 (E.D. Mo. 2013). As to Maritz's first theory, Cognizant argues only that the MSA does not impose an obligation to prevent its employees (or other unauthorized personnel) from accessing Maritz's system for improper purposes. ECF 17 at p. 11. I disagree. The obligation to "diligently perform the Outsourced Services[4] at the highest industry standards of workmanship and professionalism," and the

[4] "Outsourced Services" are defined as "project activities, tasks and services of any nature to be performed by [Cognizant] hereunder, relating to a software development project, or any other project which may be requested by Maritz, and as described in a Statement of Work." MSA § 1.4.

obligation to “keep all Confidential Information[5] strictly confidential,” both encompass a duty to prevent employees or other unauthorized personnel from accessing Maritz’s system for improper purposes. MSA §§ 4.2, 13.2.1. Maritz therefore states a valid claim for breach of contract on this basis.

Maritz’s second allegation, that Cognizant “fail[ed] to take responsibility for the security breaches,” apparently relies on a provision from the “Facilities Safety and Security” section of the MSA: “[Cognizant] shall be responsible for and shall immediately notify Maritz of, investigate and remedy any security breaches . . . at the Service Location(s).” MSA § 6.2.2. It is plausible that cybersecurity breaches are encompassed by the phrase “security breach” as contained in the MSA, and it is also plausible that the breaches originated at a Service Location, where Cognizant employees assigned to Maritz’s account were stationed. This aspect of the breach of contract count also survives dismissal.

Maritz’s third breach of contract allegation is that Cognizant failed “to prevent its employees from sharing credentials and usernames for Cognizant accounts in violation of industry standards and Maritz’s company policy.” ECF 1 at ¶ 64. Cognizant contends the MSA does not prohibit *internal* sharing of account

[5] “Confidential Information” includes “all information and proprietary materials, not generally known in the relevant trade or industry, received by either Party from the other Party in connection with any activity under or relating to this Agreement . . .” MSA § 1.1.

credentials and usernames. The MSA, however, specifically states that neither party shall disclose or release Confidential Information "to any other person," nor "use the Confidential Information of the other party for any purpose whatsoever except as expressly contemplated under this Agreement." MSA § 9.1. Maritz specifically alleges "at least one of these accounts as to which Cognizant employees shared credentials and usernames was used to hack the Maritz system in 2017." ECF 1 at ¶ 45. This is a sufficient allegation of breach.

Cognizant moves to dismiss Maritz's fourth theory, that Cognizant improperly billed Maritz for service time spent engaging in cyberattacks, arguing again that Maritz has not plausibly alleged a Cognizant employee contributed to the cyberattack. It also argues that Maritz's complaint fails to allege sufficient facts to place Cognizant on fair notice of the grounds for the claim, and that Maritz fails to establish damages resulting from the alleged breach. I have previously addressed and denied Cognizant's first argument. As to notice, Maritz identifies the MSA provision wherein Cognizant agreed all work would be "of professional quality and . . . performed in compliance with applicable laws, rules and regulations" as a plausible basis for its claim. ECF 1 at ¶ 15; MSA § 13.2.4(i). Maritz's complaint also includes the dates of the phishing attacks and gift card thefts. *See* ECF 1 at ¶¶ 26, 28, 39; ECF 21 Ex. 3. Maritz has therefore provided

Cognizant "fair notice of what [its] claim is and the grounds upon which it rests." *Swierkiewicz v. Sorema N.A.*, 534 U.S. 506, 214 (2002). Maritz has also plausibly alleged that it suffered damages as a result of payments improperly billed by Cognizant—Maritz does not need to specify the precise numerical value of damages relative to the fixed billing rate at this stage in the proceedings. *See Xpedior Creditor Tr. v. Credit Suisse First Bos. (USA) Inc*., 341 F. Supp. 2d 258, 272 (S.D.N.Y. 2004) ("Under Rule 8(a), [plaintiff] need only allege that it was damaged; it is not required to specify the measure of damages nor to plead proof of causation."). Accordingly, Cognizant's motion to dismiss Count IV is denied in full.

Count V: Negligence

To state a claim for negligence under Missouri law, the plaintiff must allege that the defendant had a duty of care to protect the plaintiff from injury, the defendant failed in performing the duty, and the defendant's failure proximately caused harm to the plaintiff. *Lopez v. Three Rivers Elec. Co-op., Inc.*, 26 S.W.3d 151, 155 (Mo. banc 2000). In Count V, Maritz alleges Cognizant owed a duty to "prevent foreseeable harm to Maritz, including taking reasonable safeguards to prevent its employees and/or third parties from using Cognizant accounts to hack Maritz's computer network," as well as a duty to "safeguard the credentials and usernames issued to Cognizant employees with access to Maritz's system." ECF 1 at ¶¶ 72, 73. Maritz alleges Cognizant breached these duties by negligently failing to hire, train and supervise its employees; allowing its employees to share account credentials; and allowing its employees or third parties to hack its computer network. *Id*. Cognizant moves to dismiss for failure to state a claim, asserting "these purported duties arose solely from the MSA . . . Maritz cannot take a bargained-for set of contractual duties and transmute them to generalized tort duties."[6] ECF 17 at pg. 19.

"Missouri law recognizes that a tort may be committed in the nonobservance of contract duties and that a negligent failure to perform a contractual undertaking may result in tort liability." *Preferred Physicians Mut. Mgmt. Grp. v. Preferred Physicians Mut. Risk Retention*, 918 S.W.2d 805, 813 (Mo. Ct. App. 1996) (citing *Howell v. Welders Prods. & Servs., Inc.*, 627 S.W.2d 311, 313 (Mo. Ct. App. 1981)). Maritz's pleadings come within the holding of this case and are sufficient to withstand dismissal.

<u>Count VI: Unjust Enrichment</u>

[6] In its reply brief, Cognizant also contends that the economic loss rule bars Maritz's negligence claim. ECF 30 at pg. 19. However, because Cognizant did not raise the argument in its memorandum in opposition, I will not consider it here. *See United States v. Vincent*, 167 F.3d 428, 431 (8th Cir. 1999) ("We do not generally consider new arguments raised in a reply brief.").

Count VI is an equitable claim for unjust enrichment brought in the alternative to the breach of contract claim. "Plaintiffs are permitted to plead both breach of contract and quasi-contract theories regardless of consistency." *Collins v. Veolia ES Indus. Servs., Inc.*, No. 4:15-CV-00743-AGF, 2015 WL 8663994, at *5 (E.D. Mo. Dec. 14, 2015); *see also Chem Gro of Houghton, Inc. v. Lewis Cnty. Rural Elec. Co-op. Ass'n.*, No. 2:11-CV-93-JCH, 2012 WL 1025001, at *3 (E.D. Mo. Mar. 26, 2012). Maritz states a valid claim for unjust enrichment.

Cognizant is correct, however, that Maritz has not sufficiently alleged a claim for an equitable accounting. "Four elements are required to establish equitable jurisdiction for an accounting: the need for discovery, the complicated nature of the accounts, the existence of a fiduciary or trust relationship and the inadequacy of legal remedies." *Shaner v. Sys. Integrators, Inc.*, 63 S.W.3d 674, 677 (Mo. Ct. App. 2001); *see also Eckel v. Eckel*, 540 S.W.3d 476, 488 (Mo. Ct. App. 2018). Maritz has not alleged any facts from which I could reasonably infer that Cognizant stood as a fiduciary or legal trustee in any capacity for Maritz—a mere 'relationship of trust' is insufficient. *See Engelsmann v. Holekamp*, 402 S.W.2d 382, 388 (Mo. 1966) (holding plaintiff must prove the existence of a fiduciary relationship to state a claim for accounting). Accordingly, to the extent

Maritz seeks to bring an independent claim for an equitable accounting, I will dismiss the claim without prejudice.

Accordingly,

IT IS HEREBY ORDERED that Cognizant's Motion to Dismiss [15] is **GRANTED** as to Maritz's Counts I, II, and III, and as to the claim for equitable accounting in Count VI; the motion is otherwise denied as to Counts IV, V, and VI.

This case will be set for a Rule 16 scheduling conference by separate order.

Catherine D Perry

CATHERINE D. PERRY
UNITED STATES DISTRICT JUDGE

Dated this 19th day of December, 2019.